

03500.017468.

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

HIROHIDE TACHIKAWA

Application No.: 10/616,941

Filed: July 11, 2003

For: NETWORK CONFIGURATION  
METHOD AND COMMUNICATION  
SYSTEM AND APPARATUS

Examiner: Not Yet Assigned

Group Art Unit: 2131

January 26, 2004

Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450

SUBMISSION OF PRIORITY DOCUMENT

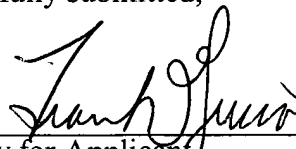
Sir:

In support of Applicant's claim for priority under 35 U.S.C. § 119, enclosed  
is a certified copy of the following foreign application:

2002-233119 filed August 9, 2002.

Applicant's undersigned attorney may be reached in our New York office by  
telephone at (212) 218-2100. All correspondence should continue to be directed to our  
address given below.

Respectfully submitted,

  
Attorney for Applicant

Registration No. 42,476

FITZPATRICK, CELLA, HARPER & SCINTO  
30 Rockefeller Plaza  
New York, New York 10112-3801  
Facsimile: (212) 218-2200  
40249v1

CFO 17468 US/kh  
10/6/6,941

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 2 年    8 月    9 日  
Date of Application:

出 願 番 号            特 願 2 0 0 2 - 2 3 3 1 1 9  
Application Number:  
[ST. 10/C]:            [ J P 2 0 0 2 - 2 3 3 1 1 9 ]

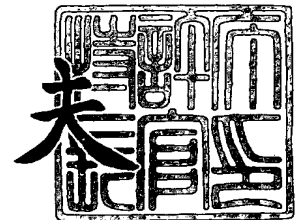
出      願      人            キヤノン株式会社  
Applicant(s):



2 0 0 3 年    8 月 1 8 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 泰



出証番号    出証特 2 0 0 3 - 3 0 6 7 1 4 0

【書類名】 特許願

【整理番号】 4771006

【提出日】 平成14年 8月 9日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/00

【発明の名称】 無線接続方法、無線接続システムおよびアクセスポイント装置

【請求項の数】 27

【発明者】

    【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社内

    【氏名】 立川 博英

【特許出願人】

    【識別番号】 000001007

    【氏名又は名称】 キヤノン株式会社

    【代表者】 御手洗 富士夫

【代理人】

    【識別番号】 100081880

    【弁理士】

    【氏名又は名称】 渡部 敏彦

    【電話番号】 03(3580)8464

【手数料の表示】

    【予納台帳番号】 007065

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9703713

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 無線接続方法、無線接続システムおよびアクセスポイント装置

【特許請求の範囲】

【請求項 1】 認証サーバ機能および認証用データの生成機能を有するアクセスポイント装置の無線接続方法において、

前記アクセスポイント装置とクライアント端末との間で、認証プロセスを必要としない第 1 の暗号化手段による無線通信のリンクを確立するステップと、

前記第 1 の暗号化手段による無線通信のリンクが確立した状態で、前記認証用データを前記クライアント端末に送付するステップと、

該認証用データを送付した後、前記第 1 の暗号化手段による無線通信のリンクを一旦破棄するステップと、

前記クライアント端末に送付された認証用データを用い、認証プロセスを必要とする第 2 の暗号化手段による無線通信に移行するステップとを有することを特徴とする無線接続方法。

【請求項 2】 前記第 1 の暗号化手段による無線通信のリンクを確立するために、前記クライアント端末から所定の入力操作を受け付けるステップを有することを特徴とする請求項 1 記載の無線接続方法。

【請求項 3】 前記所定の入力操作を、前記アクセスポイント装置に付属する表示手段、あるいは該アクセスポイント装置とネットワーク接続されたクライアント端末上で動作するブラウザに表示するステップを有することを特徴とする請求項 1 記載の無線接続方法。

【請求項 4】 前記第 1 の暗号化手段による無線通信のリンクを確立した際、前記クライアント端末の識別データを前記アクセスポイント装置に送信するステップを有することを特徴とする請求項 1 記載の無線接続方法。

【請求項 5】 前記送信された識別データを、前記アクセスポイント装置に付属する表示手段、あるいは該アクセスポイント装置とネットワーク接続されたクライアント端末上で動作するブラウザに一覧表示するステップと、

前記一覧表示された識別データに対応するクライアント端末の編集・確認を促すステップとを有し、

前記送付するステップでは、確認されたクライアント端末に対し、前記認証用データを送付することを特徴とする請求項 4 記載の無線接続方法。

【請求項 6】 前記一覧表示されたクライアント端末の確認が終了した場合、該確認されたクライアント端末固有の識別情報を、前記アクセスポイント装置内のアドレスフィルタに自動設定するステップを有し、

前記アドレスフィルタへの自動設定により、前記確認されたクライアント端末以外のアクセスポイント装置への接続を禁止し、所定の復帰手順がとられない限り、前記接続の禁止状態を維持することを特徴とする請求項 5 記載の無線接続方法。

【請求項 7】 前記所定の入力操作はアクセスポイント識別情報の入力であり、該アクセスポイント識別情報は前記第 2 の暗号化手段による無線通信に移行する際にも使用されることを特徴とする請求項 2 記載の無線接続方法。

【請求項 8】 前記認証用データは認証サーバ用証明書データであることを特徴とする請求項 1、2、5 または 7 記載の無線接続方法。

【請求項 9】 認証サーバ機能および認証用データの生成機能を有するアクセスポイント装置とクライアント端末との間で無線通信を行う無線接続システムにおいて、

前記アクセスポイント装置と前記クライアント端末との間で、認証プロセスを必要としない第 1 の暗号化手段による無線通信のリンクを確立する確立手段と、

前記第 1 の暗号化手段による無線通信のリンクが確立した状態で、前記認証用データを前記クライアント端末に送付する送付手段と、

該認証用データを送付した後、前記第 1 の暗号化手段による無線通信のリンクを一旦破棄する破棄手段と、

前記クライアント端末に送付された認証用データを用い、認証プロセスを必要とする第 2 の暗号化手段による無線通信に移行する移行手段とを備えたことを特徴とする無線接続システム。

【請求項 10】 前記第 1 の暗号化手段による無線通信のリンクを確立するために、前記クライアント端末から所定の入力操作を受け付ける受付手段を備えたことを特徴とする請求項 9 記載の無線接続システム。

【請求項 11】 前記所定の入力操作を、前記アクセスポイント装置に付属する表示手段、あるいは該アクセスポイント装置とネットワーク接続されたクライアント端末上で動作するブラウザに表示する表示制御手段を備えたことを特徴とする請求項 9 記載の無線接続システム。

【請求項 12】 前記第 1 の暗号化手段による無線通信のリンクを確立した際、前記クライアント端末の識別データを前記アクセスポイント装置に送信する送信手段を備えたことを特徴とする請求項 9 記載の無線接続システム。

【請求項 13】 前記送信された識別データを、前記アクセスポイント装置に付属する表示手段、あるいは該アクセスポイント装置とネットワーク接続されたクライアント端末上で動作するブラウザに一覧表示する第 2 の表示制御手段と

、  
前記一覧表示された識別データに対応するクライアント端末の編集・確認を促す督促手段とを備え、

前記送付手段は、確認されたクライアント端末に対し、前記認証用データを送付することを特徴とする請求項 12 記載の無線接続システム。

【請求項 14】 前記一覧表示されたクライアント端末の確認が終了した場合、該確認されたクライアント端末固有の識別情報を、前記アクセスポイント装置内のアドレスフィルタに自動設定する自動設定手段を備え、

前記アドレスフィルタへの自動設定により、前記確認されたクライアント端末以外のアクセスポイント装置への接続を禁止し、所定の復帰手順がとられない限り、前記接続の禁止状態を維持することを特徴とする請求項 13 記載の無線接続システム。

【請求項 15】 前記所定の入力操作はアクセスポイント識別情報の入力であり、該アクセスポイント識別情報は前記第 2 の暗号化手段による無線通信に移行する際にも使用されることを特徴とする請求項 10 記載の無線接続システム。

【請求項 16】 前記認証用データは認証サーバ用証明書データであることを特徴とする請求項 9、10、13 または 15 記載の無線接続システム。

【請求項 17】 認証サーバ機能および認証用データの生成機能を有し、クライアント端末との間で無線通信を行うアクセスポイント装置において、

前記クライアント端末との間で、認証プロセスを必要としない第 1 の暗号化手段による無線通信のリンクを確立する確立手段と、

前記第 1 の暗号化手段による無線通信のリンクが確立した状態で、前記認証用データを前記クライアント端末に送付する送付手段と、

該認証用データを送付した後、前記第 1 の暗号化手段による無線通信のリンクを一旦破棄する破棄手段と、

前記クライアント端末に送付された認証用データを用い、認証プロセスを必要とする第 2 の暗号化手段による無線通信に移行する移行手段とを備えたことを特徴とするアクセスポイント装置。

【請求項 18】 前記第 1 の暗号化手段による無線通信のリンクを確立するために、前記クライアント端末から所定の入力操作を受け付ける受付手段を備えたことを特徴とする請求項 17 記載のアクセスポイント装置。

【請求項 19】 前記所定の入力操作を、付属の表示手段、あるいはネットワーク接続されたクライアント端末上で動作するブラウザに表示する表示制御手段を備えたことを特徴とする請求項 17 記載のアクセスポイント装置。

【請求項 20】 前記第 1 の暗号化手段による無線通信のリンクを確立した際、前記クライアント端末から送信された該クライアント端末の識別データを受信する受信手段を備えたことを特徴とする請求項 17 記載のアクセスポイント装置。

【請求項 21】 前記受信した識別データを、付属の表示手段、あるいはネットワーク接続されたクライアント端末上で動作するブラウザに一覧表示する第 2 の表示制御手段と、

前記一覧表示された識別データに対応するクライアント端末の編集・確認を促す督促手段とを備え、

前記送付手段は、確認されたクライアント端末に対し、前記認証用データを送付することを特徴とする請求項 20 記載のアクセスポイント装置。

【請求項 22】 前記一覧表示されたクライアント端末の確認が終了した場合、該確認されたクライアント端末固有の識別情報を、前記アクセスポイント装置内のアドレスフィルタに自動設定する自動設定手段を備え、



前記アドレスフィルタへの自動設定により、前記確認されたクライアント端末以外のアクセスポイント装置への接続を禁止し、所定の復帰手順がとられない限り、前記接続の禁止状態を維持することを特徴とする請求項 21 記載のアクセスポイント装置。

【請求項 23】 前記所定の入力操作はアクセスポイント識別情報の入力であり、該アクセスポイント識別情報は前記第 2 の暗号化手段による無線通信に移行する際にも使用されることを特徴とする請求項 18 記載のアクセスポイント装置。

【請求項 24】 前記認証用データは認証サーバ用証明書データであることを特徴とする請求項 17、18、21 または 23 記載のアクセスポイント装置。

【請求項 25】 複数の無線通信方式に対応するため、無線通信拡張インターフェースを少なくとも 1 つ備え、該無線通信拡張インターフェースに、所望の無線通信方式に対応した無線通信拡張カードを装着することによって、前記所望の無線通信方式で前記クライアント端末との無線通信を実現することを特徴とする請求項 17 記載のアクセスポイント装置。

【請求項 26】 前記無線通信拡張インターフェースと、基幹ネットワークに接続するためのインターフェースとを別々に備え、前記無線通信拡張インターフェースに接続されたクライアント端末と前記基幹ネットワークとのルーティング処理を行うことを特徴とする請求項 25 記載のアクセスポイント装置。

【請求項 27】 ルーティング処理を行う CPU と同一の CPU で、前記認証サーバ機能および前記認証用データの生成機能を実現することを特徴とする請求項 26 記載のアクセスポイント装置。

#### 【発明の詳細な説明】

#### 【0001】

#### 【発明の属する技術分野】

本発明は、無線 LAN (IEEE 802.11) や Bluetooth 等の無線通信機能を有する端末を用いて、安全な Personal Area Network (PAN) を構築する場合などに用いられる無線接続方法、無線接続システムおよびアクセスポイント装置に関する。

**【0002】****【従来の技術】**

従来、無線LANやBluetoothでは、その通信媒体として電波を用いるので、通信先の制限が難しかった。このため、これらの規格では、通信先毎に暗号鍵を変更することで、たとえパケットをのぞき見られても、それを解読できないようにするといった防御手段がとられてきた。現在、最も一般的な無線通信暗号化手段は、IEEE 802.11方式の場合、WEPキー（40bit, 128bit）による暗号化であり、Bluetooth方式の場合、Pinコードから自動生成される128bitの暗号鍵（128bit）による暗号化である。

**【0003】**

しかし、これらの暗号化方式は脆弱性を有することが指摘されており、無線通信の安全性を更に高めるための暗号化方式として、802.11方式では、802.1xベースの認証を実施した上での動的WEPキー変換（EAP）や、TKIP, AESといった更に高度な暗号化方式、Bluetooth方式では、802.1xベースの上位アプリケーション層での認証・暗号化方式などが検討され、一部実施されている。

**【0004】**

この中でも802.1xをベースとしたEAP（Extensible Authentication Protocol、拡張可能認証プロトコル）方式と呼ばれる認証・暗号化手段は、一部のOS環境において、802.11方式向けの認証・暗号化手段として標準で実装されている。

**【0005】**

無線LAN（802.11）におけるEAP方式では、クライアントの端末がネットワーク接続要求を行う際、TCP/IPを利用してイントラネット内に設けられた認証サーバ（RADIUSサーバ等）とデータ通信を行い、認証サーバからクライアントへの証明書の要求またはチャレンジを実施する。

**【0006】**

クライアントは、証明書所有の証明を行うか、チャレンジに対してアカウント

名とパスワードを返し、それらが認証サーバ内のデータと一致した場合、認証サーバは、無線通信を暗号化するための 128 bit の暗号鍵または暗号鍵生成手段を、アクセスポイントおよびクライアントに返す。このようなプロセスを経て、クライアントが認証をパスすると、それ以降の無線通信は、クライアントとアクセスポイントとの両者間で、128 bit の暗号鍵を WEP キーとして利用することで、暗号化される。さらに、上記プロセスは一定時間毎に定期的に実施され、暗号鍵の更新が行われる。

#### 【0007】

また、Bluetooth 方式では、PAN プロファイルにおいて、セキュリティ向上のために、802.1x 認証・暗号化手段を用いることが推奨されている。Bluetooth の場合、無線媒体である電波を暗号化するための鍵の生成は、Bluetooth 方式で通信を行うデバイス間の Pin コードによる相互認証によって自動的に行われるので、認証サーバから受け取った暗号鍵情報を、無線 LAN における WEP キーのように、電波そのものの暗号化鍵として利用できないが、無線媒体としての電波を生成する前段階で、パケットを暗号化する際の鍵として利用できる。これにより、二重に暗号化して通信のセキュリティを向上させることができる。

#### 【0008】

このように、802.1x 方式の認証・暗号化プロセスでは、認証を実施するための認証サーバがネットワーク内に存在し、同サーバでクライアントのアカウントを集中管理する。このため、802.1x 方式を用いることで、クライアントがどこにいても、認証サーバとの TCP/IP による通信が実施可能である限り、同一のアカウント・パスワードを用いてイントラネット等のネットワークに接続することができる。

#### 【0009】

##### 【発明が解決しようとする課題】

しかしながら、上記従来の無線接続システムでは、上記 802.1x 方式による認証・暗号化プロセスを用いることで、クライアントは無線通信による安全なネットワーク接続を実現できるが、このために、ネットワーク内に認証サーバを

設置し、かつこの認証サーバに予めクライアントのアカウントを登録しておく必要がある。

#### 【0010】

すなわち、802.1x方式は、比較的規模の大きなイントラネット等における運用を想定した方式であり、無線によるネットワーク接続を行うクライアントも、認証サーバ上にアカウントを持ったメンバに限定されるという制限があった。

#### 【0011】

このため、認証サーバにアカウントの無い外来者が参加するミーティングを行う場合、あるいはイントラネットへの接続手段がない社外の会議室等でのミーティングを行う場合、802.1x方式による認証・暗号化プロセスを利用した無線通信による安全なネットワーク構築ができないという不具合があった。

#### 【0012】

尚、このような場合、認証・暗号化を無くした無線通信を行うことは実現可能であるが、セキュリティの面から大きな問題があることは勿論である。また、手作業による無線通信用パラメータの設定を実施するようにした場合、無線通信の暗号化は可能であるが、クライアントはイントラネット内で通常利用する802.1x方式のアカウント・パスワードの入力による自動接続とは、全く異なる接続手段を手動で行わなければならない、操作方法に統一性が無く、煩雑であり、利便性が損なわれる。

#### 【0013】

そこで、本発明は、802.1x認証・暗号化方式などの認証プロセスを要する、比較的安全性の高い暗号化方式による無線通信を用いたPAN構築を、認証プロセスに対応したアカウントや証明書を事前に所有していないクライアント端末においても実現可能である無線接続方法、無線接続システムおよびアクセスポイント装置を提供することを目的とする。

#### 【0014】

##### 【課題を解決するための手段】

上記目的を達成するために、本発明の無線接続方法は、認証サーバ機能および

認証用データの生成機能を有するアクセスポイント装置の無線接続方法において、前記アクセスポイント装置とクライアント端末との間で、認証プロセスを必要としない第1の暗号化手段による無線通信のリンクを確立するステップと、前記第1の暗号化手段による無線通信のリンクが確立した状態で、前記認証用データを前記クライアント端末に送付するステップと、該認証用データを送付した後、前記第1の暗号化手段による無線通信のリンクを一旦破棄するステップと、前記クライアント端末に送付された認証用データを用い、認証プロセスを必要とする第2の暗号化手段による無線通信に移行するステップとを有することを特徴とする。

#### 【0015】

本発明の無線接続システムは、認証サーバ機能および認証用データの生成機能を有するアクセスポイント装置とクライアント端末との間で無線通信を行う無線接続システムにおいて、前記アクセスポイント装置と前記クライアント端末との間で、認証プロセスを必要としない第1の暗号化手段による無線通信のリンクを確立する確立手段と、前記第1の暗号化手段による無線通信のリンクが確立した状態で、前記認証用データを前記クライアント端末に送付する送付手段と、該認証用データを送付した後、前記第1の暗号化手段による無線通信のリンクを一旦破棄する破棄手段と、前記クライアント端末に送付された認証用データを用い、認証プロセスを必要とする第2の暗号化手段による無線通信に移行する移行手段とを備えたことを特徴とする。

#### 【0016】

本発明のアクセスポイント装置は、認証サーバ機能および認証用データの生成機能を有し、クライアント端末との間で無線通信を行うアクセスポイント装置において、前記クライアント端末との間で、認証プロセスを必要としない第1の暗号化手段による無線通信のリンクを確立する確立手段と、前記第1の暗号化手段による無線通信のリンクが確立した状態で、前記認証用データを前記クライアント端末に送付する送付手段と、該認証用データを送付した後、前記第1の暗号化手段による無線通信のリンクを一旦破棄する破棄手段と、前記クライアント端末に送付された認証用データを用い、認証プロセスを必要とする第2の暗号化手段

による無線通信に移行する移行手段とを備えたことを特徴とする。

#### 【0017】

##### 【発明の実施の形態】

本発明の無線接続方法、無線接続システムおよびアクセスポイント装置の実施の形態について図面を参照しながら説明する。

#### 【0018】

##### [第1の実施形態]

図1は第1の実施形態におけるアクセスポイント装置およびクライアント端末によって構築されるネットワークシステムを示す図である。図において、1はIEEE802.11やBluetooth等の規格を用いた無線通信手段により、安全なネットワークを構築するアクセスポイントである。2はアクセスポイント1に内蔵された無線通信部である。3はアクセスポイント1に内蔵された認証サーバである。4はアクセスポイント1に内蔵された証明書サーバである。5はアクセスポイント1からクライアント端末へのメッセージを表示する表示部である。

#### 【0019】

6はIEEE802.11やBluetooth等の無線通信手段である。7、8はアクセスポイント1と無線接続されるPDAである。9、10はアクセスポイント1と無線接続されるノートPCである。

#### 【0020】

図2はアクセスポイント1の構成を示すブロック図である。図において、101はCPUである。102はメモリコントローラやバス変換機能を有するノースブリッジチップである。103はノースブリッジチップ102から出力される高速バスを更に低速の汎用バスに変換するサウスブリッジである。

#### 【0021】

104はRAMである。105は表示用グラフィックチップである。106は表示装置である。表示用グラフィックチップ105および表示装置106は図1の表示部5を構成する。107はプログラムや様々な設定情報を記憶するROMである。108、109はPCIバスからCardbus等の標準拡張バスへの

変換を行うブリッジチップである。110、111、112、113は無線通信拡張カードを挿入することによって様々な無線通信方式に対応する拡張バスインターフェースである。

#### 【0022】

114はカスケード接続用MAC (Media Access Control) である。115はカスケード接続用PHY (Physical layer) である。116はカスケード接続用802.3uインターフェースである。117は有線ネットワークによるPAN構築用MACである。118は有線ネットワークによるPAN構築用スイッチングコントローラである。119、120、121、122は有線ネットワークによるPAN構築用インターフェースである。123は上記回路に電源を供給する電源装置である。

#### 【0023】

拡張バスインターフェース110、111、112、113は全て同等の機能を有しており、このインターフェースに無線通信機能を有する拡張カードを挿入することによって、拡張カードはアクセスポイントとして機能する。また、複数の拡張バスインターフェースを装備し、Bluetooth、802.11b、802.11a等それぞれに異なる無線通信手段に対応した無線通信拡張カードを挿入することで、1台で複数の無線通信手段に同時に対応可能なアクセスポイントを構築することができる。さらに、同一の通信手段に対応した無線通信拡張カードを複数挿入すると、1枚の無線通信拡張カードで対応可能なユーザ数を越えた数のユーザに、1台のアクセスポイント装置で対応することができる。また、アクセスポイントを経由して基幹ネットワークに接続する無線通信のクライアント端末に対し、ユーザ毎のルーティングやフィルタリングを行うことで、不正なアクセスを相互に禁止できる。さらに、単一のCPU101およびその周辺回路で、アクセスポイントのルーティング機能、認証サーバ機能、および認証サーバ用アカウントあるいは証明書生成機能（証明書サーバ機能）を実現することで、製品化する場合のコストを低減できる。

#### 【0024】

図3はアクセスポイント装置のソフトウェアの構成を示す図である。認証サー

バ (RADIUSサーバ等) のエミュレーション機能やアクセスポイントを実現するためのTCP/IPスタック等を、図2の本体側ブロック (Main Board) に設けることによって、種類の異なる無線通信手段への対応を柔軟に行い、かつシステムの総コストを抑えることができる。

#### 【0025】

つぎに、上記構成を有するアクセスポイント1を利用し、無線通信によるPANを構築する動作を示す。無線通信によるPANを構築する際、アクセスポイント1に対する起動操作か、あるいは何らかのスイッチ入力を行うと、アクセスポイント1は、低レベルな暗号化を施した無線接続を確立するために必要な情報を、表示部5に表示する。このときの表示は、ESS ID、WEPキー、あるいはPinコード等の802.11やBluetoothによる無線通信を暗号化するためのパラメータそのものでもよい。また、ユーザが所有するクライアント端末7、8、9、10に、予めインストールされたプログラムによって、上記無線通信を暗号化するためのパラメータに自動変換を行うためのキーワードであってもよい。

#### 【0026】

図4は802.11方式による無線接続を確立する処理手順を示すフローチャートである。まず、前述したように、新しいPANの構築要求が、アクセスポイント1の起動やスイッチ入力によって行われるまで待機し (ステップS1)、PANの構築要求が行われた場合、アクセスポイント1は、802.11方式による低レベルの暗号化を施した無線通信に必要なパラメータであるESS IDとWEPキーを表示する (ステップS2)。

#### 【0027】

ここで、PANに接続しようとするユーザは、これらの表示されたパラメータを、各自が所有するクライアント端末7、8、9、10に手入力する。この操作によって、低レベルな暗号化を施した無線通信が、アクセスポイント1とクライアント端末7、8、9、10との間に確立される。

#### 【0028】

尚、このとき、TCP/IPベースの接続を確立する必要があるので、低レベ



ルの暗号化を施した無線レベルでのリンクが確立した後、アクセスポイント 1 に内蔵された DHCP 機能等を用い、各クライアント端末 7、8、9、10 は、IP アドレスの自動発行等の処理を行い、TCP/IP によるネットワーク接続を確立する。

#### 【0029】

その後、アクセスポイント 1 は、自身に無線接続されているクライアント端末 7、8、9、10 の情報を、アクセスポイント 1 の表示部 5 に一覧表示する（ステップ S3）。このとき表示されるクライアント端末の情報は、接続されている無線端末のハードウェア識別コードでもよいが、その場合、PAN の管理責任者は、不正アクセス者の特定等のために、各クライアント端末の持つハードウェア識別コードを事前に把握しておく必要がある。

#### 【0030】

しかし、ハードウェア識別コードの管理は、ユーザにとって非常に煩雑である。そこで、PAN を構築しようとするユーザは、事前に自身が所有するクライアント端末 7、8、9、10 に、PAN 構築を支援するためのソフトウェアをインストールしておき、このとき、クライアント端末利用者の氏名や所属などの個人識別情報を入力しておくものとする。このような処理を施しておき、低レベルの暗号化を施した無線接続を確立した際、各クライアント端末 7、8、9、10 からアクセスポイント 1 に個人識別情報を送信することによって、アクセスポイント 1 は、自身に無線接続されているクライアント端末 7、8、9、10 の個人識別情報を一覧表示することができる。

#### 【0031】

図 5 は個人識別情報の一覧表示を示す図である。PAN の管理責任者は、無線通信によって接続されているユーザの一覧表示を見ながら、任意に編集し、不正な PAN 参加者がいないことを目視で確認すると、アクセスポイント 1 に対し、PAN 参加者の確認作業が完了したことを示すためのスイッチ入力等を行う。すなわち、ステップ S3 で無線接続されているクライアント端末 7、8、9、10 の個人識別情報を一覧表示した後、修正要求があるか否かを判別し（ステップ S4）、修正要求がある場合、修正作業を行って（ステップ S5）、ステップ S3

の処理に戻る。一方、修正要求がないとして、確認作業完了が入力された場合、そのままステップ S 6 の処理に移行する。

#### 【0032】

アクセスポイント 1 は、確認作業完了が入力された場合、確認されたユーザ以外の P A N 参加を拒絶するため、確認されたユーザの M A C アドレス等を用いたハードウェア識別コードによるフィルタリング設定を行う（ステップ S 6）。尚、このフィルタリング設定は、一般的な無線 L A N アクセスポイントが有する M A C アドレスによるユーザ制限機能を用いることにより、確認されたユーザ名の M A C アドレスを自動設定する等の処理で実現できる。

#### 【0033】

また、アクセスポイント 1 は、同時に確認済みの全てのクライアント端末に対する認証用アカウントまたは証明書の発行作業を行う（ステップ S 7）。全てのクライアント端末に認証用アカウントまたは証明書を送信し（ステップ S 8）、送信が完了したか否かを判別する（ステップ S 9）。送信が完了すると、アクセスポイント 1 は、一旦、現状の低レベルな暗号化を施した無線通信によるリンクを破棄し（ステップ S 10）、認証処理を要する高レベルな暗号化を施した無線通信の開始に備え、本処理を終了する。

#### 【0034】

クライアント端末 7、8、9、10 は、低レベルの暗号化を施した無線通信によるリンクが破棄された後、リンク中に受信した認証用アカウントまたは証明書を利用して、E A P 等の認証プロセスを要する比較的高レベルな暗号化を施した無線通信を実施するための接続プロトコルを自動的に開始する。

#### 【0035】

尚、このとき、クライアント端末 7、8、9、10 は、前回の比較的低レベルな暗号化を施した無線通信によるリンクを行った場合と同一の E S S I D を用いて、E A P 等の認証プロセスを要する比較的高レベルな暗号化を施した無線通信への移行を行う。これは、認証用アカウントまたは証明書の発行を行ったアクセスポイント 1 に、クライアント端末 7、8、9、10 を確実に誘導して接続するためである。

## 【0036】

図6はEAPによる認証を行う際、クライアント端末7、8、9、10、アクセスポイント1内の無線通信部2、アクセスポイント1内の認証サーバ3の遷移を示す図である。クライアント端末7、8、9、10は、アクセスポイント1内の無線通信部2を介してアクセスポイント1内の認証サーバ3に2回のEAP-Response(200、201)を送信する。

## 【0037】

これにより、アカウントとパスワードのセット、または証明書データの送信を行い、自身が認証サーバに登録されているクライアント端末であることの認証を行う。その結果、認証に合格すると、クライアント端末のネットワークアクセスが許可され、その後、クライアント端末7、8、9、10とアクセスポイント1内の無線通信部2との間に設定されるWEPキーを、一定時間毎に動的に変更することで、比較的高レベルな暗号化を施した無線通信を実現することができる。

## 【0038】

尚、第1の実施形態では、アクセスポイント1の表示部5を利用し、比較的低レベルの暗号化を施した無線接続を実施する際のIDやCode等のキーワード表示、PAN参加者の編集時の一覧表示などを実施する旨の記述を行ったが、この表示は、有線ネットワークによるPAN構築用インターフェース119、120、121、122に接続されたクライアントデバイスに、WEBブラウザを利用して間接的に表示することも可能である。この場合、アクセスポイント1に表示部や入力用スイッチなどを具備する必要が無くなるので、コスト削減に有効である。

## 【0039】

## [第2の実施形態]

前記第1の実施形態では、新規にPANを構築する際の動作について示したが、第2の実施形態では、実際にPANを構築する際の動作として、会議を例に挙げ、会議開催時のPANに必要とされる機能の観点から説明する。

## 【0040】

ここで、会議開催時にクライアント端末を相互に接続するPANを構築する場

合、前記第1の実施形態で示したように、比較的高レベルな暗号化を施した無線接続を利用することは、ユーザの利便性の点から非常に好ましい。

#### 【0041】

会議用PANを構築する場合、各ユーザに発行するアカウントや証明書は、恒久的なものではなく、会議中だけ一時的に有効なものであることが必要である。このため、会議用にアクセスポイントを用いる場合、図4のステップS1で新しいPANの構築要求があった後、ステップS2の処理を行う前に、PAN管理責任者による会議予定時間の入力ステップ処理を追加する。

#### 【0042】

この入力処理を追加することで、アカウントの有効時間を認証サーバに設定したり、発行する証明書の有効時間を証明書内のパラメータとして反映させることで、認証プロセスを要する比較的高レベルの暗号化を施した無線接続によるPANに有効時間を与えることができる。

#### 【0043】

また、前記第1の実施形態で示したように、PANの管理責任者による確認作業が終了すると、PANは、MACアドレスフィルタリング等の処理によってロック状態となり、新たなユーザ参加を認めなくなる。

#### 【0044】

しかし、アクセスポイント1を会議等の環境下で用いる場合、一旦、ロック状態とした後、遅刻者の追加等の理由により、クライアント端末を追加するケースが考えられる。このような場合、PANの管理責任者が、遅刻者を視認した際、アクセスポイント1を直接操作するか、あるいは管理責任者が使用しているクライアント端末9のWEBブラウザを利用してアクセスポイント1の管理画面を起動し、間接的にアクセスポイント1を操作して、ロック状態を解除する。

#### 【0045】

図7は第2の実施形態における個人識別情報の一覧表示を示す図である。この画面上には、図5の画面と比べ、「ロック解除」ボタン31が設けられている。この「ロック解除」ボタン31をクリックすることにより、PANのMACアドレスフィルタによる参加制限が解除される。

## 【0046】

また、このとき、PAN管理責任者は、遅刻者に対し、図中、Keywordとして表示されるIDやCode情報を伝える。ここでは、Keywordは「GC Smeet」である。この後、追加でPANに参加しようとするユーザは、自身の所有するクライアント端末でアプリケーションを起動し、Keywordを入力する。ここで入力するキーワードは、前記第1の実施形態で示したように、比較的低レベルの暗号化を施した無線接続を実施する際、各ユーザが入力するESS ID、WEPキー、あるいはPinコード等の802.11やBluetoothによる無線通信を暗号化するためのパラメータそのものでもよい。本実施形態では、最終的にそれらのパラメータに自動変換されるキーワードが用いられている。

## 【0047】

図8は第2の実施形態における802.11方式による追加クライアントの無線接続を確立する処理手順を示すフローチャートである。ロック解除要求が行われたか否かを判別する（ステップS11）。ロック解除要求が行われた場合、アクセスポイント1は、802.11方式による低レベルの暗号化を施した無線通信に必要なパラメータであるESS IDとWEPキーを表示する（ステップS12）。

## 【0048】

クライアント端末にキーワードを入力すると、このクライアント端末は、既にその他のユーザによってPANが形成されているアクセスポイントに対し、低レベルの暗号化が施された無線接続を試みる。アクセスポイント1は、PANに追加・参加しようとするクライアント端末を認識すると、画面表示を更新し、追加参加ユーザの個人情報を一覧に追記する（ステップS13）。

## 【0049】

尚、この追記は、図7の「更新」ボタン32がクリックされたときに行われてもよい。PAN管理責任者は、更新された一覧表示を確認し、仮に、不正ユーザが表示された場合、編集作業を行い、不正ユーザを削除する。すなわち、修正要求があるか否かを判別し（ステップS14）、修正要求がある場合、修正作業を

行って（ステップS15）、ステップS13の処理に戻る。一方、修正要求がないとして、確認作業完了が入力された場合、ステップS16の処理に移行する。

#### 【0050】

前記第1の実施形態と同様、アクセスポイント1は、確認作業完了の入力が行われた場合、確認されたユーザ以外のPAN参加を拒絶するため、確認されたユーザのMACアドレス等を用いたハードウェア識別コードによるフィルタリング設定を更新する（ステップS16）。また、アクセスポイント1は、同時に新たに確認された追加クライアント端末に対し、認証用アカウントまたは証明書の発行作業を行う（ステップS17）。

#### 【0051】

追加クライアント端末に認証用アカウントまたは証明書を送信し（ステップS18）、送信完了を待つ（ステップS19）。送信が完了すると、アクセスポイント1は、追加クライアント端末に対し、現状の低レベルな暗号化を施した無線通信によるリンクを破棄し（ステップS20）、認証処理を要する高レベルな暗号化を施した無線通信の開始に備え、本処理を終了する。

#### 【0052】

尚、遅刻者のPANへの追加作業を実施する際、その他のPAN参加者は、継続的に認証プロセスを要する比較的高レベルな暗号化を施した無線接続を維持しており、そのPAN上で作業を継続できることは言うまでもない。

#### 【0053】

また、追加クライアント端末は、低レベルの暗号化を施した無線通信によるリンクが破棄された後、リンク中に受信した認証用アカウントまたは証明書を利用し、EAP等の認証プロセスを要する比較的高レベルな暗号化を施した無線通信を行うための接続プロトコルを自動的に開始する。このとき、追加クライアント端末は、前回の比較的低レベルな暗号化を施した無線通信によるリンクを行った場合と同一のESS IDを用いて、アクセスポイント1と選択的に接続することは言うまでもない。

#### 【0054】

これにより、前記第1の実施形態と同様、追加クライアント端末は、アクセス

ポイント 1 内の無線通信部 2 を介してアクセスポイント 1 内の認証サーバ 3 に 2 回の E A P - R e s p o n s e ( 2 0 0 、 2 0 1 ) を送信することによって、アカウントとパスワードのセットまたは証明書データの送信を行い、自身が認証サーバに登録されているクライアント端末であることの認証を行う。

#### 【 0 0 5 5 】

この結果、認証に合格すると、追加クライアント端末のネットワークアクセスが許可され、その後、一定時間毎に、W E P キーを動的に変更することで、比較的高レベルな暗号化を施した無線通信を実現することができる。

#### 【 0 0 5 6 】

このように、認証プロセスを要する比較的高レベルな暗号化を施した無線接続を維持しながら、同時に比較的低レベルな暗号化を施した無線接続を構築するためには、独立して暗号化レベルを制御可能な無線通信装置が必要であるが、本実施形態のように、複数の無線通信拡張カードを装着できるアクセスポイントである場合、複数の無線通信拡張カードを装着することで容易に実現することができる。

#### 【 0 0 5 7 】

また、異なる暗号化レベルによる無線通信を 1 チップで実現できるコントローラを用いる場合、アクセスポイントに複数の無線通信拡張カードを実装することなく、1 枚の無線通信拡張カードだけで第 2 の実施形態に示した処理を行うことも可能である。

#### 【 0 0 5 8 】

尚、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラムコードをシステムあるいは装置に供給することによって達成される場合にも適用できることはいうまでもない。この場合、プログラムコード自体が本発明の新規な機能を実現することになり、そのプログラム自体およびそのプログラムを記憶した記憶媒体は本発明を構成することになる。

#### 【 0 0 5 9 】

プログラムコードを供給する記憶媒体としては、ROM に限らず、例えばフレキシブルディスク、ハードディスク、CD-ROM、CD-R、DVD、不揮発

性のメモリカードなどを用いることができる。

#### 【0060】

##### 【発明の効果】

本発明によれば、アカウントや証明書を事前を取得していないユーザに対しても、認証プロセスを要する比較的高レベルな暗号化を施した無線接続システムを容易に構築できる。特に、会議等で一時的に安全なネットワークを構築したい場合に好適である。

#### 【0061】

このように、802.1x 認証・暗号化方式などの認証プロセスを要する、比較的安全性の高い暗号化方式による無線通信を用いたPAN構築を、認証プロセスに対応したアカウントや証明書を事前に所有していないクライアント端末においても実現可能である。

#### 【0062】

また、PAN構築の際に利用する無線通信手段を簡単に選択できる。さらに、PAN構築の際、無線通信手段を複数同時に利用可能とし、異なる無線通信手段で構成されたPANを簡単に構築することである。また、1枚のカードで対応できるユーザ数を越えたクライアント数によるPANの構築やクライアントの負荷分散を実現できる。したがって、PANに参加可能な無線通信手段におけるクライアントの総数を増加させることができる。

#### 【0063】

さらに、無線通信手段によって構築したPANを、イントラネットやインターネットなどの基幹ネットワークに接続する場合、不正なアクセスを相互に禁止することができる。また、本アクセスポイントを製品化する場合のコストを低減できる。

#### 【0064】

さらに、アカウントや証明書を事前に所有していないクライアント端末によって、認証プロセスを要する比較的安全性の高い暗号化方式を用いた無線通信によるPANを構築する際、クライアントの操作を容易にすることができる。また、アカウントや証明書を事前に所有していないクライアント端末と、アクセスポイ



ントを接続する際のアクセスポイント側の設定操作を容易にすることができる。

#### 【0065】

また、構築された無線通信によるPANのクライアントに矛盾がないか否かの最終確認手段を提供できる。さらに、無線通信によるPANに参加可能なクライアント条件が、確認後に無断で変更できないようにすることができる。したがって、無線通信によるPANに対するクライアントの追加を無断で実行できないようにすることができる。また、認証プロセスを要する比較的高レベルな暗号化手段による無線通信へ移行する際、そのクライアントに対する認証を実施可能なアクセスポイントへ選択的に無線接続することができる。

#### 【図面の簡単な説明】

##### 【図1】

第1の実施形態におけるアクセスポイント装置およびクライアント端末によって構築されるネットワークシステムを示す図である。

##### 【図2】

アクセスポイント1の構成を示すブロック図である。

##### 【図3】

アクセスポイント装置のソフトウェアの構成を示す図である。

##### 【図4】

802.11方式による無線接続を確立する処理手順を示すフローチャートである。

##### 【図5】

個人識別情報の一覧表示を示す図である。

##### 【図6】

EAPによる認証を行う際、クライアント端末7、8、9、10、アクセスポイント1内の無線通信部2、アクセスポイント1内の認証サーバ3の遷移を示す図である。

##### 【図7】

第2の実施形態における個人識別情報の一覧表示を示す図である。

##### 【図8】

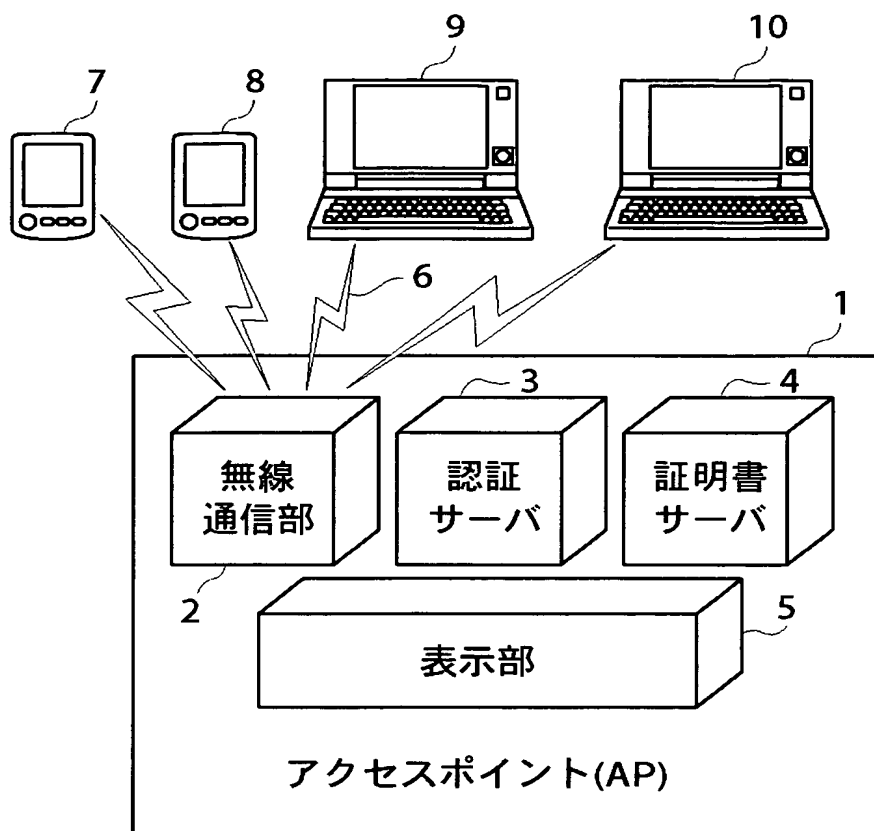
第 2 の実施形態における 8 0 2 . 1 1 方式による追加クライアントの無線接続を確立する処理手順を示すフローチャートである。

【符号の説明】

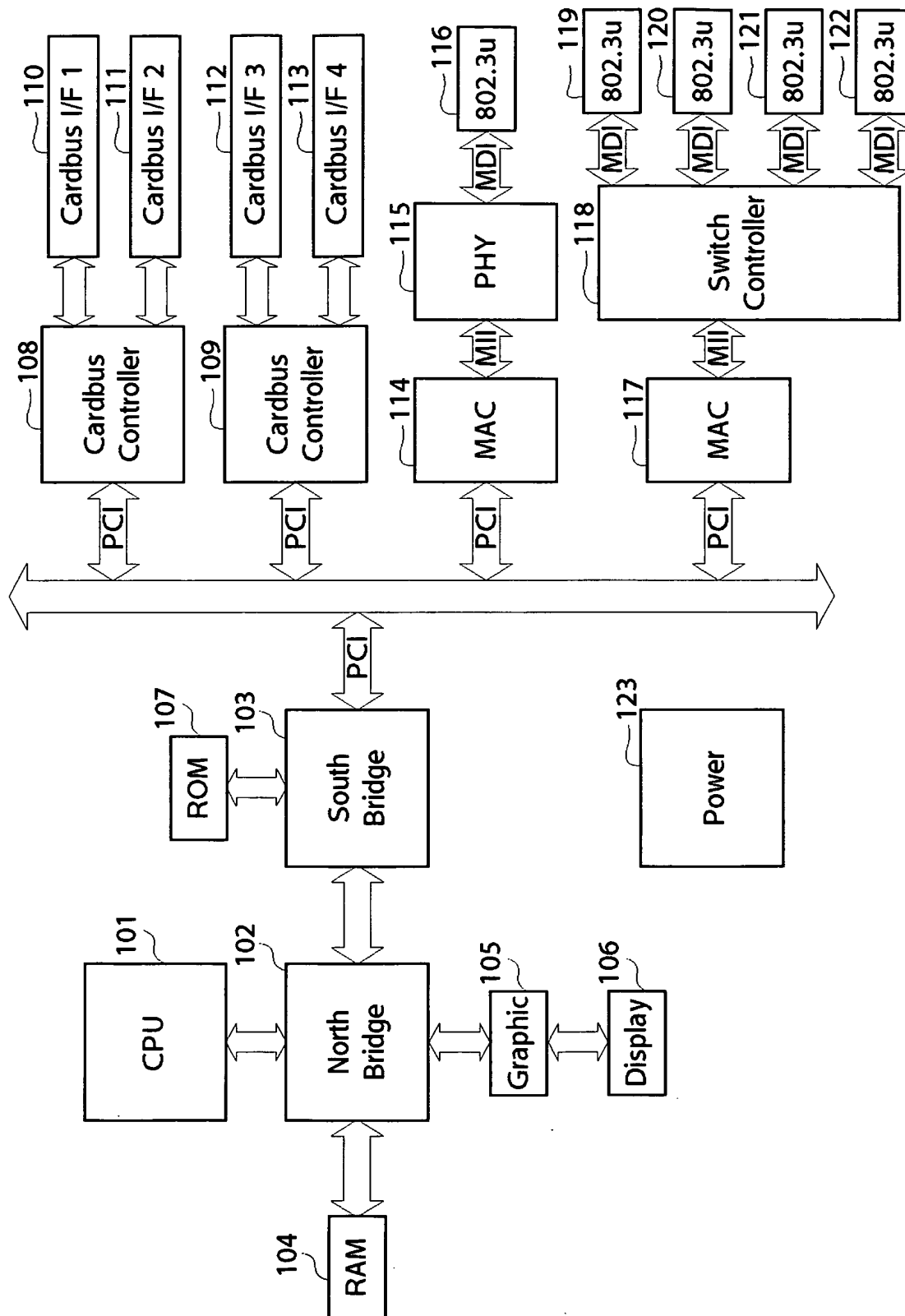
- 1    アクセスポイント装置
- 2    無線通信部
- 3    認証サーバ
- 4    証明書サーバ
- 7、8    P D A
- 9、1 0    P C
- 1 0 1    C P U
- 1 1 0 ～ 1 1 3    拡張バスインターフェース
- 1 1 9 ～ 1 2 2    P A N 構築用インターフェース

【書類名】 図面

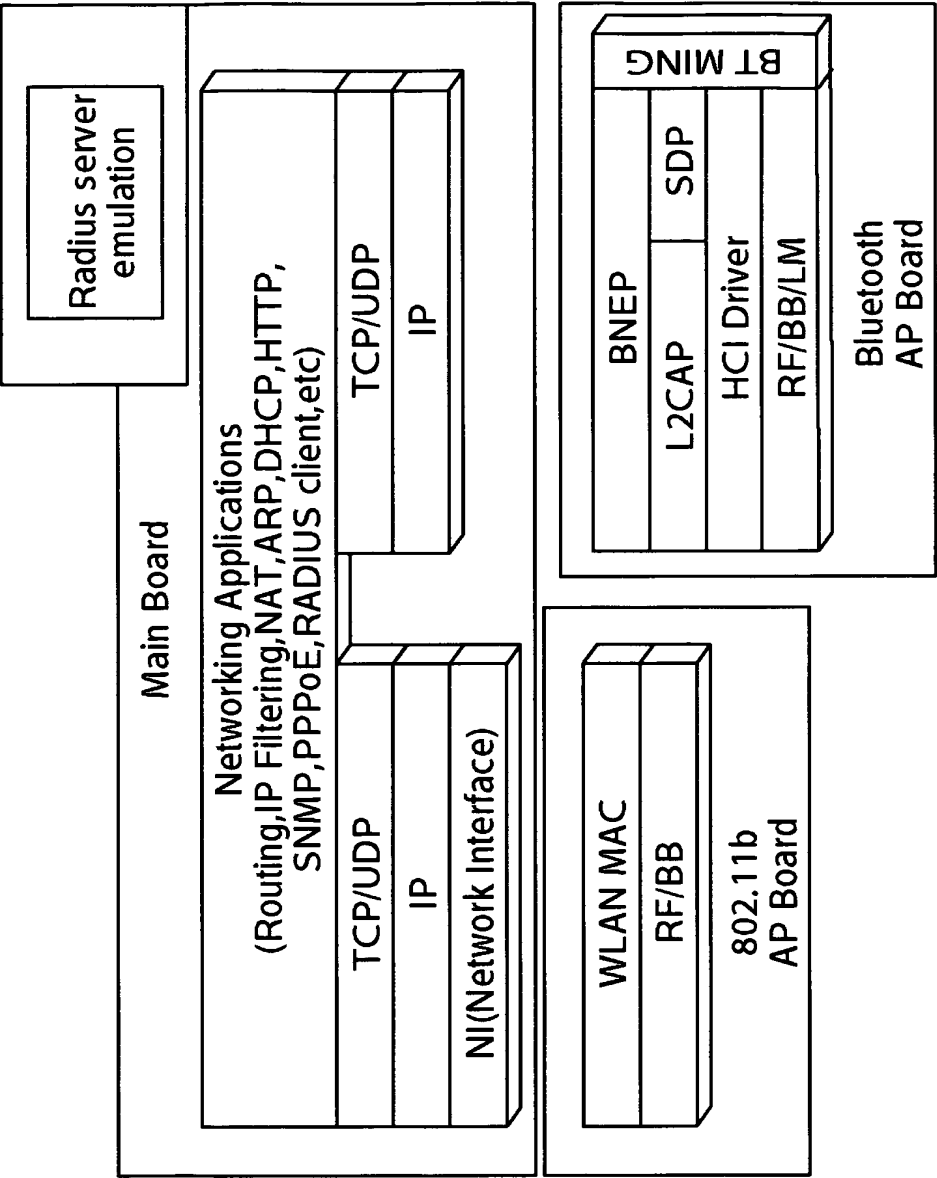
【図 1】



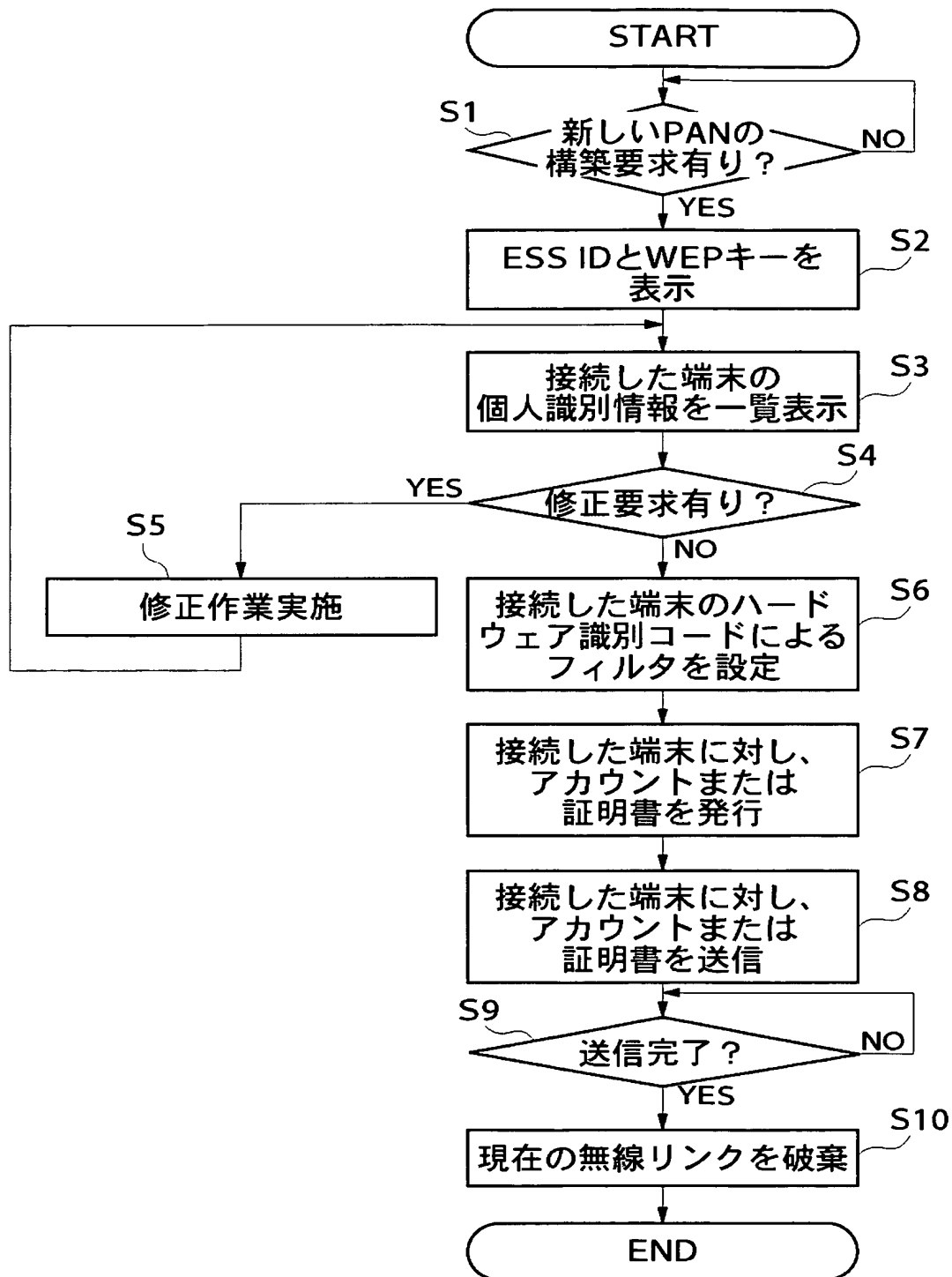
【図 2】



【図 3】



【図4】



【図 5】

氏名	社名	所属	役職
鈴木 一郎	×××××	第53開発室	室長
佐藤 次郎	×××××	開発企画課	課長代理
斉藤 三郎	X商事	第2販売課	主任
伊藤 史	X商事	第2販売課	
中井 八郎	×××××	第53開発室	
松田 綾	×××××	開発企画課	
David Martin	IT Corp.	sales	Manager

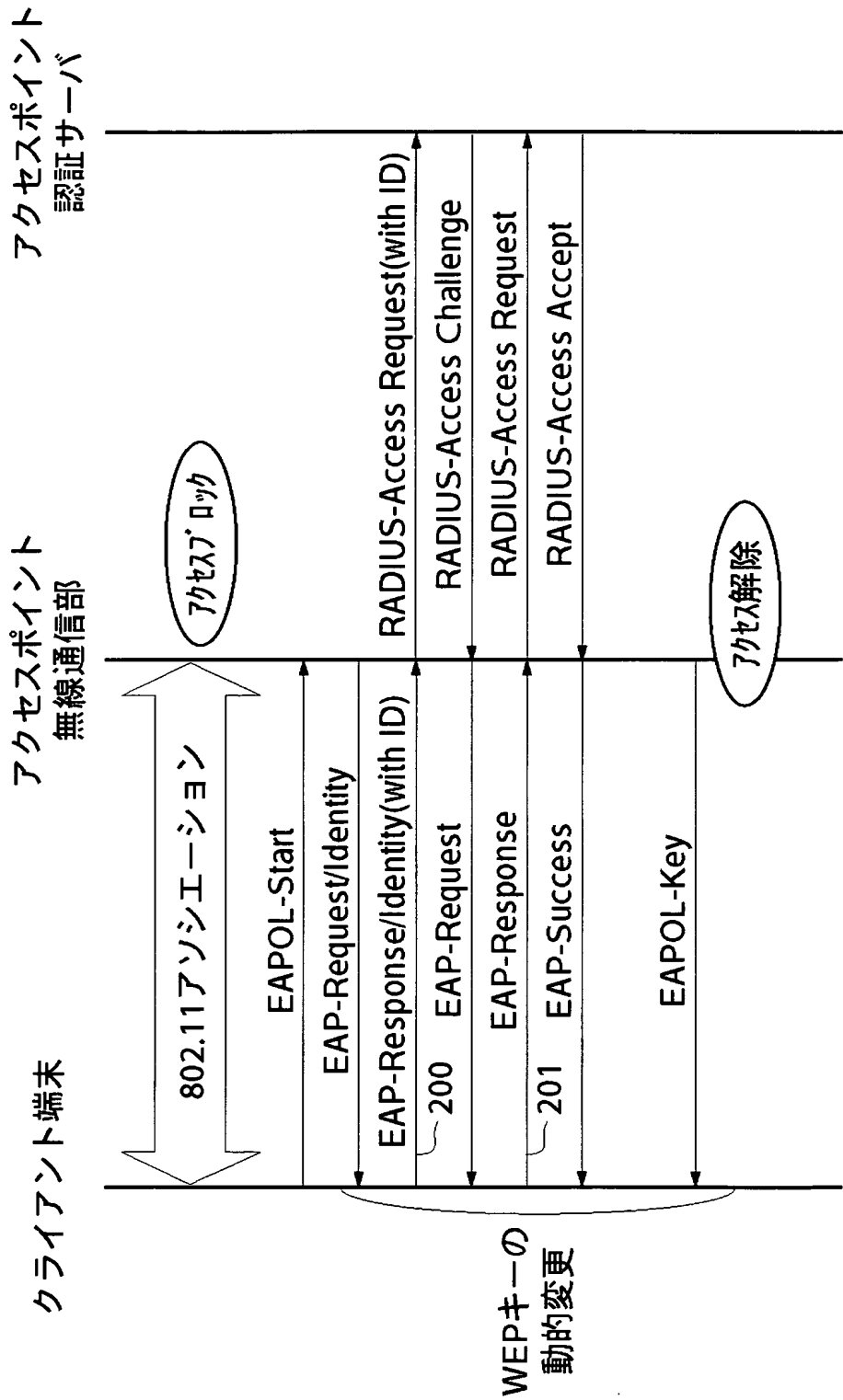
Keyword : GCSmeet

更新

削除

確認

【図 6】





【図 7】

氏名	社名	所属	役職
鈴木 一郎	××××	第53開発室	室長
佐藤 次郎	××××	開発企画課	課長代理
斉藤 三郎	X商事	第2販売課	主任
伊藤 史	X商事	第2販売課	
中井 八郎	××××	第53開発室	
松田 綾	××××	開発企画課	
David Martin	IT Corp.	sales	Manager

Keyword : GCSmeet

ロック解除

更新

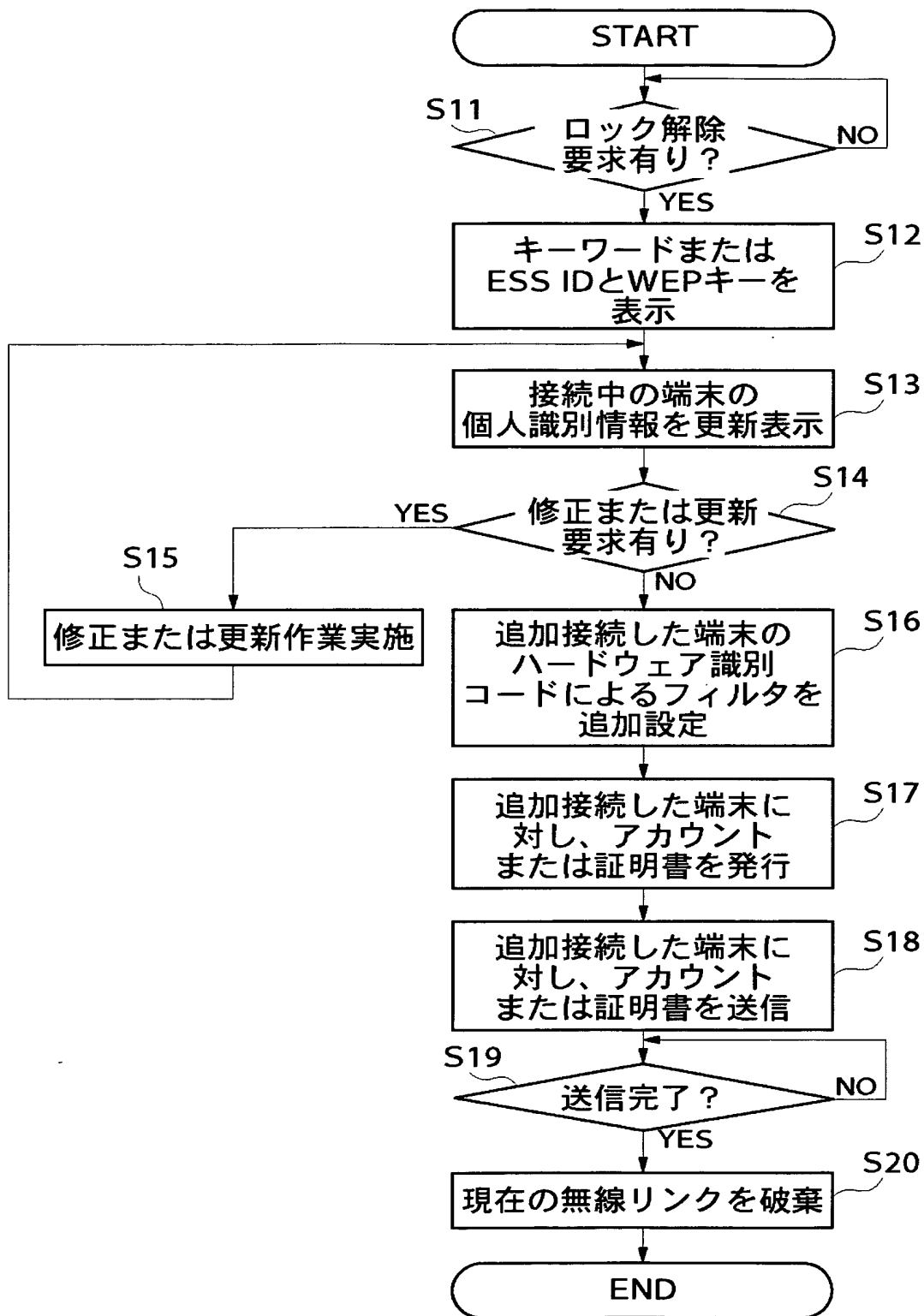
削除

確認

31

32

【図 8】



【書類名】 要約書

【要約】

【課題】 比較的安全性の高い暗号化方式による無線通信を用いた P A N 構築を、認証プロセスに対応したアカウントや証明書を事前に所有していないクライアント端末においても実現可能であるアクセスポイント装置を提供する。

【解決手段】 比較的低レベルな暗号化方式による無線通信のリンクをクライアント端末との間で確立した後、認証プロセスを必要とする高レベルな暗号化方式による無線通信を行うために必要な認証用データをクライアント端末に送信し、一旦リンクを破棄する。再度、認証用データを用いて安全な無線通信による P A N を再構築する。

【選択図】 図 1

特願 2 0 0 2 - 2 3 3 1 1 9

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 1 0 0 7 ]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都大田区下丸子 3 丁目 3 0 番 2 号

氏 名

キヤノン株式会社